Datenschutz im Internet

MODUL 06

verbraucherzentrale

SMART SURFER

Fit im digitalen Alltag

Lernhilfe für aktive Onliner*innen

Ministerium für Umwelt, Landwirtschaft,
Natur- und Verbraucherschutz
des Landes Nordrhein-Westfalen

Gebündelte Kompetenz rund um die Themen: Datensicherheit, Verbraucherschutz, Digitalisierung, Unterhaltung und digitale Ethik

Seit 2011 bietet das medienpädagogische Ausbildungskonzept „Silver Surfer – Sicher online im Alter“ eine digitale Grundbildung für aktive Onliner*innen. 2020 wurde das Konzept neu aufgelegt. Dafür sind einzelne Themenbereiche erheblich erweitert und einige neue hinzugefügt worden. Zusätzlich wurde auch der Titel der Lernhilfe angepasst: „Smart Surfer – Fit im digitalen Alltag“.

Die Lernhilfe „Smart Surfer – Fit im digitalen Alltag“ wurde gemeinsam von Mitarbeiter*innen der Verbraucherzentrale Rheinland-Pfalz e.V., der Medienanstalt Rheinland-Pfalz, des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz und der Stiftung MedienKompetenz Forum Südwest sowie der Clearingstelle Medienkompetenz der Deutschen Bischofskonferenz an der Katholischen Hochschule Mainz erstellt.

verbraucherzentrale Rheinland-Pfalz

medienanstalt rlp LMK

Der Landesbeauftragte für den DATENSCHUTZ und die INFORMATIONSFREIHEIT Rheinland-Pfalz

MKFS MEDIEN KOMPETENZ FORUM SÜDWEST STIFTUNG

Katholische Hochschule Mainz – Clearingstelle Medienkompetenz

Herausgeber der Lernhilfe „Smart Surfer“ in Nordrhein-Westfalen ist das Ministerium für Umwelt, Landwirtschaft, Natur- und Verbraucherschutz des Landes Nordrhein-Westfalen.

Das Projekt wird gefördert durch:

RheinlandPfalz – Ministerium für Familie, Frauen, Jugend, Integration und Verbraucherschutz

Bayerisches Staatsministerium für Umwelt und Verbraucherschutz

Baden-Württemberg – Ministerium für ländlichen Raum und Verbraucherschutz

Ministerium für Umwelt, Landwirtschaft, Natur- und Verbraucherschutz des Landes Nordrhein-Westfalen

LAND BRANDENBURG – Ministerium für Soziales, Gesundheit, Integration und Verbraucherschutz

LFK: Die Medienanstalt für Baden-Württemberg

Wie Sie diese Lernhilfe benutzen

Die Lernhilfe „Smart Surfer – Fit im digitalen Alltag“ bietet viele Informationen rund um das Thema Internet. Sie soll gleichzeitig als Nachschlagewerk dienen.

Seit dem Jahr 2020 wird die Lernhilfe in digitaler Form angeboten. Sie können die PDF-Dateien zu den einzelnen Modulen über Ihren PC/Laptop sowie Ihr Tablet nutzen.

In einer PDF-Datei können Sie gezielt nach Stichwörtern suchen. Mit einem Klick auf eine Internetadresse gelangen Sie direkt auf die jeweilige Website, vorausgesetzt, Sie lesen dieses PDF über ein internetfähiges Gerät. Natürlich können Sie sich diese PDF-Datei ausdrucken. Weitere Informationen zum Thema „Wie nutze ich ein PDF?“ finden Sie unter:
www.silver-tipps.de/was-bedeutet-eigentlich-pdf

Die Lernhilfe „Smart Surfer – Fit im digitalen Alltag“ besteht aus 9 Modulen:

- Modul 1: Was ist das Internet?
- Modul 2: Wie man das Internet nutzt
- Modul 3: Unterhaltungsmöglichkeiten im Internet
- Modul 4: Wie man Risiken im Netz vermeidet
- Modul 5: Die Welt des mobilen Internets
- **Modul 6: Datenschutz im Internet**
- Modul 7: Kommunikation im Netz
- Modul 8: Soziale Medien im Netz
- Modul 9: Ein Blick in die Zukunft des Internets

Mehr Informationen zum Projekt „Smart Surfer“ und alle PDF-Dateien zum Download finden Sie unter: *www.verbraucherzentrale-rlp.de/smart-surfer*

Alle Informationen der Lernhilfe haben wir nach bestem Wissen und Gewissen geprüft.
Wir freuen uns stets über kritische Anmerkungen, die helfen, diese Lernhilfe noch besser zu machen. Sie möchten Kritik äußern? Dann zögern Sie nicht, uns zu kontaktieren (per E-Mail an: telekommunikation@vz-rlp.de).

In der Lernhilfe finden sich unterschiedliche Symbole:

Weiterführendes: Das entsprechende Thema wird an einer anderen Stelle der Lernhilfe erneut aufgegriffen und umfangreicher dargestellt.

Silver Tipps: Auf der Onlineplattform www.silver-tipps.de finden sich viele weiterführende Informationen rund um das Thema Sicherheit im Internet.

Link: Über die eingefügten Links sind weiterführende Informationen und andere Internetquellen zum Thema zu finden.

Fakt: Interessante Fakten werden im Text gesondert hervorgehoben.

Paragraf: Wer sich im rechtlichen Bereich weiterführend informieren will, findet an dieser Stelle die genauen Gesetzesbezeichnungen.

Begriffe, die mit einem Pfeil (») markiert sind, werden im Anschluss an den Text in einem Glossar näher erläutert.

Gender-Hinweis: Gendergerechte Sprache ist ein wichtiges Thema. Deshalb wurde in der Lernhilfe mit der Gender-Schreibweise des Ministeriums für Familie, Frauen, Jugend, Integration und Verbraucherschutz Rheinland-Pfalz gearbeitet und das Gender-Sternchen (*) genutzt, um alle Leser*innen gleichermaßen anzusprechen.

Vorwort

Sehr geehrte Damen und Herren,

für viele Menschen gehört das Internet zum Lebensalltag. Die digitale Welt bietet vielfältige Möglichkeiten, etwa um sich zu informieren, einzukaufen oder soziale Kontakte zu pflegen. Auch der Alltag wird durch „smarte“ Anwendungen vereinfacht – Einkäufe, Bankerledigungen oder das Buchen von Bus- und Zugtickets erfordern mit mobilen Endgeräten nur wenige Klicks.

Ein souveräner Umgang mit dem Internet und seinen zahlreichen, sich ständig verändernden Angeboten ist aber keine Selbstverständlichkeit – insbesondere für ältere Menschen. Es braucht aktuelles, praxisorientiertes Wissen und eine Informationsvermittlung, welche Ratsuchende genau dort abholt, wo sie gerade stehen.

Und genau hier setzt der Smart Surfer an, indem die Lernhilfe die Lebensrealität älterer Menschen in den Blick nimmt. Ob digitale „Neueinsteigende“, die bisher nur wenig Berührungspunkte mit dem Netz haben, oder Menschen, die sich vertieft mit einem bestimmten Thema beschäftigen möchten – sie alle werden praxisorientiert durch verschiedene Bereiche der digitalen Welt begleitet und für Gefahren und Chancen im Netz sensibilisiert.

Besonders am Herzen liegt mir das Thema Datenschutz und Datensouveränität. Die Wahrnehmung von Datenrechten stellt Verbraucherinnen und Verbraucher unabhängig ihres Alters vor große Herausforderungen. Die Auswahloptionen bei der Verarbeitung persönlicher Daten und die Konsequenzen der Auswahl sind nur unzureichend bekannt. Ich freue mich, dass der Datenschutz mit Modul 6 ein eigenes Kapitel erhält und auch in den weiteren Modulen immer wieder Informationen zu diesem zentralen Verbraucherschutzthema integriert wurden.

Bei der Überarbeitung der Lehrmaterialien wurde die Zielgruppe auf Verbraucherinnen und Verbraucher ab 50plus erweitert. Der Smart Surfer adressiert u. a. Basiswissen zum Aufbau einer Webseite oder zur Videotelefonie – aber auch ganz aktuelle Themen wie Fake News oder die Debatte um Algorithmen und Künstliche Intelligenz. Alles Themen, die ganz sicher auch für die „jüngeren Älteren“ einen großen Mehrwert bieten. Deshalb bin ich überzeugt davon, dass wir mit dem Smart Surfer-Angebot den generationsübergreifenden Dialog zu digitalen Themen weiter stärken und ausbauen können. Darin sehe ich einen großen Mehrwert für unsere Gesellschaft und die Möglichkeit für alle Beteiligten, sich online wie offline als informierte und souveräne Verbraucherinnen und Verbraucher zu bewegen.

Ich freue mich, dass Nordrhein-Westfalen Teil des Smart Surfer-Projekts geworden ist und von den hochwertigen Lehrmaterialen profitieren kann. Ich wünsche Ihnen eine spannende Lektüre!

Ihre

Ursula Heinen-Esser
Ministerin für Umwelt, Landwirtschaft, Natur- und Verbraucherschutz des Landes Nordrhein-Westfalen

MODUL
06

Datenschutz im Internet

Datenschutz ist ein komplexes Thema und wird in Öffentlichkeit und Politik intensiv diskutiert. Neue Technologien und die umfassende Nutzung des → Internets machen es nahezu unvermeidbar, dass jede*r von uns Datenspuren hinterlässt. Nicht zuletzt die Einführung der europäischen Datenschutz-Grundverordnung brachte die öffentliche Diskussion erneut ins Rollen. Das Thema Datenschutz wird immer umfangreicher, besonders im Hinblick auf Fragen der Privatsphäre und der Menge an Daten, die täglich ins Netz geladen werden.

Doch warum ist Datenschutz heute so wichtig? Welche Daten werden im Netz gesammelt und von wem zu welchem Zweck genutzt? Und was passiert eigentlich mit den Daten von Verstorbenen? Das und mehr erfahren Sie im Modul 6.

6.1 Die Debatte um den Datenschutz

Durch neue Technologien und die voranschreitende Digitalisierung vieler Lebensbereiche gewinnt das Thema Datenschutz für uns alle an Bedeutung. Das gesamtgesellschaftliche Interesse an diesem vielschichtigen Themenkomplex ist groß. Die Wirtschaft zum Beispiel möchte ihre Kund*innen besser kennenlernen, sie an sich binden und Produkte optimieren, die Werbeindustrie will Produkte möglichst zielgenau und ohne Streuverluste bewerben, Haftpflichtversicherungen möchten ihre Risiken mindern und Tarife entsprechend der Fahrweise oder Hobbys von Versicherten anbieten, Internetanbieter wollen Klickzahlen erhöhen, um Werbeeinnahmen zu generieren, und Strafverfolgungsbehörden möchten für Ermittlungen oder zur Gefahrenabwehr auf digitale Kommunikationsdaten zugreifen.

1983: Hinführung zum Grundrecht auf informationelle Selbstbestimmung

Nach der Debatte um die Volkszählung im Jahr 1983 führte das Bundesverfassungsgericht im Dezember 1983 auf Grundlage des Allgemeinen Persönlichkeitsrechts das Grundrecht auf informationelle Selbstbestimmung ein. Dieses Recht besagt, dass alle Bürger*innen das Recht haben, über Preisgabe und Verwendung ihrer personenbezogenen Daten selbst zu bestimmen.

Europäische DSGVO: https://s.rlp.de/9Md8h

Seit Mai 2018 gilt die europäische Datenschutz-Grundverordnung (DSGVO) als europaweit einheitlicher Rechtsrahmen für den Datenschutz. An die Datenschutzregeln der EU müssen sich alle Unternehmen (auch aus Nicht-EU-Staaten) halten, die in Europa ihre Dienste anbieten oder Waren verkaufen.

Modul 5.4: Persönliche Daten und Datenschutzrechte im Internet

Das Thema Datenschutz ist sehr komplex. Auch in Deutschland wird über eine sinnvolle Balance zwischen Datenschutz, dem Recht auf Meinungs- und Pressefreiheit sowie den Eingriffsbefugnissen von Behörden für die Gefahrenabwehr und Strafverfolgung diskutiert. Aktuell ist hier viel in Bewegung. Denn aufgrund der technischen Entwicklung sowie der zunehmenden Digitalisierung vieler Lebensbereiche werden immer mehr personenbezogene Daten digital erfasst, verarbeitet und gespeichert. Das angemessene Verhältnis von Freiheit und Sicherheit muss deswegen ständig neu austariert werden. Ein wichtiges Korrektiv sind hierbei die Gerichte, die in den vergangenen Jahren Urteile zu den verschiedenen Themen gesprochen haben (zum Beispiel zu den Themen Vorratsdatenspeicherung und Online-Durchsuchung) und damit den rechtlichen Rahmen abstecken.

Neben den gesetzlichen Rahmenbedingungen ist die Entwicklung der Technik ein entscheidender Faktor bei Fragen des Datenschutzes. Die rasante Entwicklung im IT- und Kommunikationssektor bringt immer wieder neue Technologien und Anwendungen auf den Markt. Oft werden Daten erhoben, ohne dass Nutzer*innen darüber informiert werden. Die Kontrolle über die Weitergabe und Verwendung der eigenen Daten wird damit immer schwieriger.

Das Internet kennt keine Landesgrenzen, das Datenschutzrecht schon. Dies führt dazu, dass für einzelne Websites unterschiedliche Datenschutzrichtlinien gelten können, je nachdem, von wo aus eine Seite betrieben wird und wer darauf zugreift. Viele Websites fallen beispielsweise unter US-amerikanisches Recht, weil sie in den USA bereitgestellt oder „gehostet“ werden. Das heißt nichts anderes, als dass der Server, auf dem die Daten zu dieser Website gespeichert sind, in diesem Land steht. Hier hat die seit 2018 geltende Datenschutz-Grundverordnung (DSGVO) eine wesentliche Änderung gebracht: Die DSGVO legt nach ihrem „Marktortprinzip“ fest, dass ihre Regelungen auch dann gelten, wenn außereuropäische Anbieter Nutzer*innen in der Europäischen Union elektronische Dienste anbieten oder Waren wie zum Beispiel eine App digital vertreiben.

2018: Einführung der Datenschutz-Grundverordnung (DSGVO)

Die Frage, welche Rechte Nutzer*innen haben, spielt eine immer größere Rolle bei Kauf- und Nutzungsentscheidungen. Denn Nutzer*innen wollen wissen, wie vertraulich ihre Daten behandelt werden und wie ihre Privatsphäre geschützt wird. Datenschutz ist in Zeiten einer digitalen und globalisierten Wirtschaft auch Teil der Wirtschaftspolitik. Zu ihren Aufgaben gehört auch, Monopolanbietern wie Facebook, Google, WhatsApp oder anderen außereuropäischen Marktriesen im Interesse der Nutzer*innen und zum Erhalt von Privatsphäre und Verbraucherschutz die Stirn zu bieten.

Privatsphäre und Öffentlichkeit

In der Diskussion um den Datenschutz stellt sich immer auch die Frage nach dem Verhältnis von Privatsphäre und Öffentlichkeit. Der Privatraum des und der Einzelnen ist ein schützenswertes Gut, das ihm und ihr durch das Grundgesetz zugesichert ist. Angesichts mancher Fernseh- und Interneteindrücke beginnt man sich jedoch zu fragen, inwieweit Privatsphäre heute noch eine Rolle spielt. Sendungen wie

„Big Brother“ oder Pseudo-Dokusendungen wie „We are Family“ liefern den Zuschauer*innen einen tiefen Einblick in die Privatsphäre anderer Menschen, ebenso wie zahlreiche Bilder und Videos, die Internetnutzer*innen ins Netz hochladen. Dabei sollte man sich aber immer die Frage stellen: Entspricht dieses Bild der Realität? Ist es authentisch? Oder ist das eine von Produktionsfirmen und Schauspieler*innen inszenierte Welt, ein inszeniertes Bild von Alltag?

Weitergabe nutzerbezogener Daten

Zwischen Medienunternehmen und Wirtschaft besteht ein enges Abhängigkeitsverhältnis. Insbesondere die Medienunternehmen des privaten Rundfunks, wie private Fernsehsender, leben von ihren Werbeeinnahmen. Allein deshalb haben sie ein Interesse daran, mit Wirtschaftsunternehmen zusammenzuarbeiten. Die Medien liefern die notwendigen Daten, um die Werbung stärker auf Zielgruppen und die Bedürfnisse Einzelner zu fokussieren. Und die Wirtschaft zahlt für diese Informationen. Dies zeigt, dass Privatsphäre oder deren Wert im Einzelfall unterschiedlich aufgefasst werden können. Mit Blick auf die zunehmende Digitalisierung fast aller Lebensbereiche sollte jedoch immer bedacht werden, wo und wie viel man von sich preisgibt.

6.2 Datensammler

Es mag einem vielleicht seltsam vorkommen, dass es eine andere Person interessieren könnte, welche Bücher man im Internet kauft oder welche von anderen hochgeladenen Fotos man mag. Diese Daten sind jedoch oft die Währung, mit der man im Internet – auch bei kostenfreien Angeboten – „bezahlt“. Indem Daten von Nutzer*innen gesammelt und ausgewertet werden, wird beispielsweise individuelle Werbung geschaltet. Darüber hinaus können Vorlieben von Personengruppen erkannt und Profile über die Bewegung von Nutzer*innen im Internet erstellt werden und vieles mehr.

Marktmacht durch Daten

Fast jede*r erwachsene Deutsche hat schon einmal bei Amazon bestellt (Stand 2020). Rund 60 Millionen Deutsche nutzen täglich den zu Facebook gehörenden Messenger-Dienst WhatsApp. Die 70 Prozent der Smartphone-Besitzer*innen, die ein Gerät mit dem Betriebssystem Android haben, kommen an einem Google-Konto kaum vorbei. Die meisten der übrigen Smartphone-Nutzer*innen haben ein Apple-Gerät. Damit sind Daten von nahezu allen in Händen der vier großen US-amerikanischen IT-Giganten Google, Apple, Facebook und Amazon. Diese Unternehmen haben eins gemeinsam: ihre Marktmacht, die vor allem durch das Sammeln von Massen an Daten ihrer Nutzer*innen zustande kommt.

60 Millionen Deutsche nutzen WhatsApp täglich.

Beispiel Amazon

Amazon hat in Deutschland nicht nur einen großen Kundenkreis und eine Palette von 229 Millionen Produkten im Angebot (Stand 2020). Die Kund*innen werden durch ein spezielles Angebot, die sogenannte „Prime"-Mitgliedschaft, bei der für einen Jahresbeitrag von 69 Euro unter anderem jede Bestellung versandkostenfrei geliefert wird, stark an Amazon gebunden. Mehr als 17 Millionen solcher Prime-Mitgliedschaften bestehen in Deutschland.

Zugleich hält Amazon mit einer derart breiten Produktpalette, zahlreichen Händler*innen und einer Vielzahl an Bestellungen einen unglaublichen Datenschatz in Händen, der fleißig genutzt wird. Zum einen werden die Such- und Bestellhistorien ausgewertet, um den Kund*innen immer zielgenauere Kaufempfehlungen zu machen. Der Algorithmus, der hinter den Empfehlungen steckt, schlägt ihnen dabei nicht nur etwa nach dem Kauf einer Sporthose den Kauf von Turnschuhen vor, er weiß aus vorangegangenen Käufen auch, ob er Ihnen hochwertigere oder günstigere Modelle anbieten muss, um Ihre Kauflust zu wecken. Die Monopolmacht von Amazon führt dazu, dass nahezu niemand, der in den bei Amazon vertretenen Produktkategorien seine Waren online vertreiben will, an Amazon vorbeikommt. Diese besondere Stellung nutzt Amazon und verpflichtet die Händler, die auf dem Amazon Marketplace verkaufen wollen, dazu, ihre Produkte über kein anderes Portal günstiger anzubieten. Kurz gesagt: Amazon ist nicht günstiger als die anderen, weil es einen niedrigeren Preis anbietet. Es verbietet einfach seinen Händler, an anderer Stelle günstiger zu sein.

Amazon ist nicht nur Marktplatz für die Produkte seiner Händler, es vertreibt auch Amazon-eigene Produkte. Hierfür hat es mit seiner Doppelrolle, selbst Händler und zugleich Marktplatz für seine Konkurrenzprodukte zu sein, optimale Voraussetzungen. Amazon kennt die Preise der Konkurrenz nämlich perfekt – und kann die eigene Preispolitik gezielt danach ausrichten.

Der Wert von Nutzerdaten

Neben gezielten Produktempfehlungen, die den Konsum ankurbeln sollen, dient vor allem personalisierte Werbung der Finanzierung all der scheinbar kostenlosen Angebote im Netz. Kostenlose E-Mail-Postfächer, kostenlose Routenplanung, kostenfreie Video-, Bild- oder Kommunikationsplattformen, kostenlose Vergleichsportale, kostenlose Suchmaschinen, kostenlose Enzyklopädien, kostenlose Nachrichten, kostenlose Musik usw. Einerseits handelt es sich um lauter Leistungen, für die man offline meist bezahlen muss und die man jetzt einfach so nutzen darf. Andererseits stellt sich die Frage: zu welchem eigentlichen Preis?

Beispiel Facebook

Die Werbeeinnahmen von Facebook betrugen 2019 weltweit knapp 70 Milliarden US-Dollar – das entspricht durchschnittlichen Werbeeinnahmen von 29,25 US-Dollar pro Nutzer*in. Betrachtet man nur die westliche Welt, dürfte der Betrag dort gut dreimal so hoch sein. Untersuchungen zeigen, dass sich mit verhaltensbasierter Werbung mehr als doppelt so viel einnehmen lässt wie mit pauschaler Werbung. Zur Personalisierung der Werbung nutzt Facebook 98 Datenpunkte (Stand 2016). Wenig überraschend sind dies Daten wie

- Ort,
- Alter,
- Generation,
- Geschlecht,
- Sprache,
- Bildungsniveau,
- ethnische Zugehörigkeit,
- Einkommen und Eigenkapital,
- Hausbesitz und -typ,
- Beziehungsstatus,
- Arbeitgeber.

Beispiel Facebook

Facebook interessiert sich aber auch für besondere Ereignisse und Veränderungen im Leben seiner Nutzer*innen – da diese auch Veränderungen im Konsumverhalten nach sich ziehen können. Und so analysiert Facebook

- Nutzer*innen, die innerhalb von 30 Tagen ein Jubiläum haben,
- Nutzer*innen, die von der Familie oder Heimatstadt entfernt sind,
- Nutzer*innen in Fernbeziehungen,
- Nutzer*innen in neuen Beziehungen,
- Nutzer*innen mit neuen Jobs,
- Nutzer*innen, die frisch verlobt oder verheiratet sind,
- Nutzer*innen, die vor Kurzem umgezogen sind,
- Nutzer*innen, die bald Geburtstag haben,
- Eltern und werdende Eltern.

Wie ein Dienst zu derart weitreichenden Annahmen kommt, kann man sich meist nur schwer vorstellen. Dahinter stecken oft Einzeldaten, die auf den ersten Blick banal erscheinen mögen. In der Zusammenführung mit den Daten anderer Nutzer*innen und der systematischen Speicherung und Auswertung entfalten sie ihr Überwachungspotenzial: Sind zwei Endgeräte über Nacht zumeist im selben WLAN eingewählt, spricht viel dafür, dass es sich um Familienangehörige oder Lebenspartner*innen handelt. Wer regelmäßig an Werktagen zwischen 9 und 17 Uhr im selben WLAN unterwegs ist, wird ein*e Arbeitskolleg*in sein.

Und so könnte es den Facebook-Nutzer*innen irgendwann gehen wie einer jungen Kundin einer großen US-amerikanischen Supermarktkette. Der Händler hatte 2012 aufgrund einer Analyse der gekauften Produkte (etwa bestimmter Körperpflegeprodukte und Nahrungsergänzungsmittel) erkannt, dass das Mädchen wahrscheinlich schwanger ist. Daraufhin wurden der Kundin per E-Mail Werbeangebote für Babykleidung zugesandt. Dies sah ihr Vater – und erfuhr auf diesem Weg von der Schwangerschaft seiner Teenager-Tochter.

Je nachdem, von wem welche Daten zu welchen Zwecken gesammelt werden, können die aus den Daten abgeleiteten Urteile und Bewertungen gravierende Folgen für die Betroffenen haben: Wahrscheinlich-

keitsbewertungen aufgrund der Analyse gesammelter Daten sind die Basis für Bonitätsprüfungen von Anbietern wie der Schufa, Creditreform oder Infoscore. Diese Bewertungen entscheiden dann letztlich, ob man einen Kredit oder eine Mietwohnung erhält.

Und wo bleibt der Datenschutz?

Sie selbst bestimmen über die Speicherung Ihrer Daten.

Die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten ist nur dann zulässig, wenn sie durch das Datenschutzrecht oder durch eine andere Rechtsvorschrift erlaubt ist oder eine Einwilligung der oder des Betroffenen vorliegt. Die Einwilligung ist nur wirksam, wenn sie auf freien Entscheidungen der Nutzer*innen beruht und diese vorab über den Zweck der Erhebung, Verarbeitung und Nutzung der Daten informiert wurden.

Die freiwilligen Einwilligungen der Nutzer*innen werden aber meist nicht in Kenntnis der beabsichtigen Datenerhebungen, -verarbeitungen und -nutzungen getroffen. Die seitenlangen Erläuterungen sind kompliziert und werden nur von wenigen Nutzer*innen gelesen und verstanden. Es fehlt nach wie vor an praxistauglichen Konzepten zur angemessenen Information der Nutzer*innen, damit diese, dem Idealbild der DSGVO entsprechend, wirklich informiert in die Datenverarbeitung einzuwilligen. Immer wieder zeigt sich, dass Unternehmen ungern wirklich transparent offenlegen, was sie mit Daten tun oder zu tun beabsichtigen. Und es fehlt häufig an wirklich freiwilligen und wirklich informierten Einwilligungen der Nutzer*innen.

So hat etwa der Bundesgerichtshof Mitte 2020 entschieden, dass die Nutzungsbedingungen von Facebook missbräuchlich sind. Sie lassen den Nutzer*innen keine Wahl, ob sie Facebook gestatten möchten, auch außerhalb von Facebook Daten über ihre Internetnutzung zu sammeln und zu verwenden oder nicht. Die Datensammlung geschieht für die Nutzer*innen unbemerkt zum Beispiel über andere Websites, die den „Gefällt mir“-Button von Facebook einbinden. Problematisch ist dabei nicht, dass Facebook erfährt, wenn Nutzer*innen den Button anklicken, um über Facebook zu teilen, dass ihnen ein Produkt oder ein Unternehmen gefällt. Problematisch ist, dass der eingebundene „Gefällt mir“-Button die Facebook-Nutzer*innen unter den Besucher*innen der Seite erkennt und den Besuch der Website an Facebook meldet – auch wenn die Nutzer*innen den Button gar nicht anklicken.

Staatliche Interessen

Die Macht der Daten weckt auch das Interesse von Staaten weltweit. Polizei, Strafverfolgungsbehörden und Geheimdienste möchten Zugriff auf vorhandene Datenschätze erlangen und neue Datensammlungen anlegen. Die Zwecke sind denkbar breit: von der Verfolgung schwerster Straftaten über Terrorismusbekämpfung bis zu nachrichtendienstlicher Aufklärung. Staaten wie China wird auch vorgeworfen, im Zuge der geheimdienstlichen Auslandsaufklärung gezielt Wirtschaftsspionage zugunsten chinesischer Unternehmen zu betreiben. Zudem stehen aus China stammende Produkte und Dienstleistungen, wie die Mobiltelefone von Huawei, der Bezahldienst Alipay, die sozialen Netzwerke TikTok und WeChat, unter dem Verdacht, umfassende staatliche Überwachung zu ermöglichen.

Innerhalb demokratischer Staaten ist es eine stetige Herausforderung, notwendige Eingriffsbefugnisse von Sicherheits- und Strafverfolgungsbehörden und den Schutz der Grundrechte in ein angemessenes Verhältnis zu setzen.

Ist es etwa gerechtfertigt, die Telekommunikationsdaten (wie die Rufnummer der beteiligten Anschlüsse, Zeitpunkt und Dauer eines Gesprächs sowie zugewiesene Internetadressen) aller Menschen in Deutschland für die Dauer von zehn Wochen zu speichern, ohne dass es hierfür einen konkreten Anlass gibt? Wegen dieser Datenspeicherung quasi „auf Vorrat“ wurde das Vorhaben bereits mehrfach unter dem Schlagwort „Vorratsdatenspeicherung“ diskutiert. Bemängelt wird etwa der fehlende Schutz der Kommunikation von sogenannten Berufsgeheimnisträger*innen wie Abgeordneten, Ärzt*innen, Rechtsanwält*innen, Geistlichen oder Journalist*innen.

Auch zwischen demokratischen Staaten herrscht keineswegs Einigkeit über diese Gewichtung: So enthüllte Edward Snowden 2013 ein Programm des US-amerikanischen Geheimdienstes NSA, das die umfassende Überwachung von Personen innerhalb wie außerhalb der USA anhand ihrer elektronischen Kommunikation ermöglichte. Deutschland gehört zu den Ländern, aus denen im Zuge dieser anlasslosen Überwachung ohne konkrete Verdachtsmomente besonders viele Daten gesammelt wurden.

6.3 Wann und wo werden Daten preisgegeben? Datenspuren im Internet

Bei der Bearbeitung eines Profils in einem sozialen Netzwerk wie Facebook oder bei einem Online-Einkauf ist uns meist bewusst, dass wir persönliche Daten preisgeben. Die Daten werden aktiv abgefragt, und ohne beispielsweise unsere richtige Adresse anzugeben, würde bestellte Ware kaum bei uns ankommen. Es gibt aber zahlreiche weitere Gelegenheiten, bei denen Daten von uns gesammelt und verwertet werden, auch ohne dass wir Kenntnis davon erlangen. Anhand eines beispielhaften Tagesablaufes wird deutlich, wo wir überall Daten preisgeben.

Den Daten einen Tag lang auf der Spur

Montagmorgen

Ihr Smartphone hat Sie mit Ihrem favorisierten Klingelton geweckt und noch im Bett schauen Sie nach, welche Termine heute anstehen, wie das Wetter wird und ob Ihnen jemand eine Nachricht geschickt hat.

Nach einem ausgiebigen Frühstück haben Sie beschlossen, einige Dinge an Ihrem Rechner zu erledigen. Sie fahren das Gerät hoch und gehen online. Noch bevor Sie überhaupt eine Seite aufgerufen haben, öffnet sich ein Fenster, das Sie daran erinnert, dass Ihr Antivirenprogramm ein Update benötigt. Gleichzeitig verbindet sich das Betriebssystem Ihres Rechners mit dem Server der Herstellerfirma, um ebenfalls Updates vorzunehmen. Zunächst melden Sie sich dann in Ihrem E-Mail-Programm an und entdecken die Nachricht eines Freundes, der von seinem Urlaub in Bolivien berichtet. Neben der eigentlichen E-Mail sehen Sie jetzt verschiedene Werbeangebote für Reisen nach Bolivien. Außerdem ärgern Sie sich wieder über die zahlreichen Newsletter, die Ihnen ungefragt zugegangen sind.

Nachdem Sie Ihre E-Mails gelesen haben, fällt Ihnen ein, dass Sie noch ein Geburtstagsgeschenk für Ihre Tochter benötigen. Sie sind auf der Suche nach einem Buch und gehen auf die Seite eines großen Onlineversandhandels. Da Sie diese Seite öfter besuchen und dort auch schon bestellt haben, werden Sie mit Ihrem Namen begrüßt. Bereits ein paar Tage zuvor haben Sie sich nach einem Geschenk für Ihre Tochter umgesehen, die sich sehr für Asien interessiert. Sie bekommen daher

auf Ihrer individuellen Startseite Angebote rund um das Thema Asien angezeigt. Sie durchstöbern die Angebote und finden ein geeignetes Kochbuch, das Sie aber vorerst nur auf Ihrem Wunschzettel speichern, um sich noch mit dem Rest der Familie abzustimmen.

Montagvormittag

Da Sie und Ihre Familie sich vor Kurzem einen Hund angeschafft haben, gehen Sie auf die Website Ihrer Heimatstadt und füllen dort das Onlineformular zur Anmeldung der Hundesteuer aus, das Sie dann elektronisch an die Stadt übermitteln. Sie haben sich für eine Quartalszahlung entschieden und überweisen unmittelbar nach Übertragung des Onlineformulars die erste Rate via Onlinebanking. Nachdem Sie sich auf der Seite Ihrer Bank eingeloggt haben, füllen Sie die Überweisung aus und übermitteln sie online mithilfe einer gültigen TAN. Im Anschluss daran lassen Sie Ihre Tätigkeiten im Netz zunächst ruhen und rufen Ihren Sohn auf der Arbeit an, um ihn nach seiner Meinung zu dem Kochbuch zu fragen.

*Weil das Wetter schön bleiben soll, entscheiden Sie sich, eine kurze Radtour zu machen. In der Fahrrad-App Ihres Smartphones wählen Sie eine geeignete Strecke aus. Da Sie wissen möchten, wie viele Kalorien Sie dabei verbrauchen, aktivieren Sie die Trainingsfunktion Ihrer Smartwatch, die daraufhin neben Ihren täglichen Schritten und sonstigen Aktivitäten die Zeit Ihrer Radtour, die Strecke, Geschwindigkeit, Höhenmeter, Herzfrequenz und Kalorien erfasst. Erfreut stellen Sie nach der Radtour fest, dass Sie weniger Zeit benötigt haben als der Durchschnitt der Radfahrer auf dieser Strecke. Stolz teilen Sie diese Info über WhatsApp mit Ihren Freund*innen.*

Montagmittag

Aufgrund der Radtour wird es ein wenig knapp mit dem Mittagessen. Über eine Liefer-App bestellen Sie sich daher ein leichtes Gericht aus dem vietnamesischen Restaurant in der Nähe.

Montagnachmittag

Ihre Tochter kommt überraschend zu Besuch und möchte Ihnen etwas Aufregendes im Internet zeigen. Sie hat auf Google Street View entdeckt, dass auch ihr Elternhaus im Internet zu sehen ist. Sie sind

Modul 4.4: Sicheres Onlinebanking

zunächst begeistert, werden aber nachdenklich, als Ihnen Ihre Tochter von ihren Bedenken im Hinblick auf den Datenschutz berichtet. Als Ihre Enkelin anruft, lassen Sie Ihre Tochter allein am Rechner zurück. Diese ist auf der Suche nach einer Website, an deren Namen sie sich nicht genau erinnern kann. Allerdings hat sie sie schon einmal an diesem Rechner aufgerufen, deshalb öffnet sie die Chronik beziehungsweise den Browserverlauf, also die Liste mit den zuletzt besuchten Internetseiten. Dabei stolpert Ihre Tochter auch über die Seite, auf der Sie sich zuvor das asiatische Kochbuch angesehen haben. Neugierig, ob Sie inzwischen ebenfalls die asiatische Küche für sich entdeckt haben, öffnet sie die Seite und nimmt sich vor, Sie später darauf anzusprechen.

Montagabend

Sie freuen sich darauf, sich den Spielfilm anzusehen, den Sie im Kino verpasst, aber letzte Woche mit Ihrem Digitalrecorder aufgenommen haben, als er bei einem Privatsender lief. Ärgerlich ist nur, dass er auch beim Abspielen immer wieder von Werbung unterbrochen wird, die man nicht überspringen kann. Da Ihnen die Filmmusik an einer Stelle besonders gefallen hat, achten Sie beim Nachspann auf den Titel des Stücks und sehen sich im Anschluss über die Internetfunktion des Fernsehers das entsprechende Musikvideo bei YouTube an. Schnell schauen Sie noch in der Programmvorschau, was im Lauf der Woche an Filmen kommt. Dabei fällt Ihnen eine Dokumentation über die schönsten Radwege entlang von Flüssen auf; Sie schauen sich die Informationen dazu an und merken sich die Sendung für die Aufnahme vor.

Vor dem Zubettgehen wollen Sie prüfen, ob Sie neue WhatsApp-Nachrichten erhalten haben. Tatsächlich haben einige Ihrer Freunde auf die Nachricht über Ihre Radtour reagiert und Ihnen gratuliert. Mancher hat auch Bilder oder ein Video von einer seiner Radtouren geschickt. Eine Freundin weist Sie auf eine lokale Facebook-Gruppe von Radfreunden hin. Da Sie ohnehin schauen, ob sich in Ihrem sozialen Netzwerk etwas Neues getan hat, schauen Sie kurz nach, wer in dieser Gruppe ist; einige davon kennen Sie.

Auf der Profilseite Ihres Sohnes entdecken Sie, dass er seinen Beziehungsstatus von „Single“ auf „vergeben“ geändert hat und der Gruppe „Frischer Wind in den Stadtrat Koblenz“ eingetreten ist. Sie

selbst sind in der Gruppe „Adenauer-Gymnasium Bonn – Abitur 1954“ und finden dort einen Schulkameraden, der dieser Gruppe neu beigetreten ist und den Sie lange gesucht haben. Nachdem Sie diesem Schulfreund eine Nachricht auf der Pinnwand hinterlassen haben, lesen Sie noch, dass Ihre Enkelin als ihr liebstes Hobby Tae Bo angegeben hat. Da Sie nicht wissen, worum es sich dabei handelt, geben Sie den Begriff bei einer Suchmaschine ein. Nach einigen Klicks wissen Sie, dass es sich um eine Sportart handelt, und gehen beruhigt ins Bett.

Wie viele digitale Datenspuren, schätzen Sie, haben Sie an diesem Tag im Netz hinterlassen?

Der Spruch „Das Internet vergisst nichts“ beruht auf verschiedenen Eigenschaften des Internets. Prinzipiell kann jeder Mensch, der online ist, sehen, was andere im Netz veröffentlichen. Das bedeutet Schätzungen zufolge, dass über drei Milliarden Menschen weltweit potenziell in der Lage sind, diese Daten zu sehen (Stand 2020). Je nach den individuellen Datenschutzeinstellungen betrifft das zum Beispiel den Wunschzettel bei Amazon, Blog- und Foreneinträge, Kommentare, Bewertungen oder die Daten in sozialen Netzwerken. Einmal Veröffentlichtes im Nachhinein wieder zu löschen, wäre so, „als würde man eine Tomate durch einen Ventilator werfen und hinterher versuchen, alle Stücke wieder einzusammeln“, um es mit den Worten des ehemaligen Bundesdatenschutzbeauftragten Peter Schaar auszudrücken.

„Das Internet vergisst nichts.“

Sobald Daten, seien es Videos, Fotos oder Blogeinträge, online sind, hat jede*r andere Internutzer*in Zugriff darauf und kann sie beliebig kopieren, um sie dann beispielsweise auf einer anderen Plattform zur Verfügung zu stellen. Andere Nutzer*innen kopieren die Daten wiederum von dieser Plattform und so weiter. Auf diese Weise können Daten unglaublich schnell verbreitet werden.

Datenspuren im Internet

Jedes Mal, wenn eine Internetseite aufgerufen wird, erzeugt dies eine Datenspur. Ob man bei Google, Bing oder Yahoo etwas sucht, sich ein Video ansieht oder einen Blog liest – in der Regel werden diese Aktivitäten protokolliert. Meist ist daraus nicht direkt erkennbar, welche

Person dahintersteht. Aber das kann sich schnell ändern. Im Internet wird eine Reihe von Mechanismen genutzt, um das Surfverhalten der Nutzer*innen zu erfassen. Das erregt bei vielen Besorgnis, zumindest aber Unbehagen. Der Wunsch nach Anonymität und Privatsphäre ist nichts Unanständiges. Wir bleiben im Alltag schließlich oft anonym. Zum Beispiel, wenn wir an der Kinokasse bar bezahlen, eine Zeitschrift kaufen oder eine DVD. Warum also nicht auch im Internet? Um welche Datenspuren geht es genau?

IP-Adresse

Die „**I**nternet**p**rotokoll-**Adresse**“, kurz „IP-Adresse“, wird bei jedem Klick mitgeschickt und verrät einiges über die Nutzer*innen. Oft lässt sie sich ziemlich genau dem Wohnort zuordnen oder jedenfalls der Region, aus der man kommt. In Verbindung mit den Angaben, die der Browser mitschickt, ist erkennbar, woher eine Person kommt.

IP-Adressen werden benötigt, um die Datenpakete im Internet zuzustellen. Außerdem lassen sie grundsätzlich Rückschlüsse auf die Person zu: Nicht nur der jeweilige Internetanbieter (Provider) ist in der Lage, die IP-Adresse einer bestimmten Person zuzuordnen, sondern auch jeder Anbieter einer Website, auf der sich Nutzer*innen registrieren, anmelden oder Name und Adresse hinterlassen.

Cookies

Bestellt man hin und wieder bei einem großen Onlineshop, kann es vorkommen, dass man sofort beim Aufrufen der Seite mit seinem Namen begrüßt wird. Das funktioniert über sogenannte Cookies. Das sind kleine Dateien, die auf den PCs abgelegt werden, wenn die Browsereinstellungen dies zulassen. Cookies speichern Informationen im Zusammenhang mit der jeweiligen Internetseite. Dass Cookies auf dem eigenen Rechner vorhanden sind, merkt man beispielsweise daran: Beim Ausfüllen von Onlinebestellformularen werden Daten vorgeschlagen, die man früher einmal eingegeben hat. Viele Cookies dienen dazu, Benutzerprofile anzulegen und zu verfolgen, wie sich die Nutzer*innen auf der Website bewegen, wie lange sie bleiben und was sie sich näher anschauen. Technisch notwendige Cookies, zum Beispiel für einen Warenkorb, sind jedoch in der Regel unproblematisch.

Häufig werden Cookies dabei nicht allein von der konkret aufgerufenen Webseite gesetzt, sondern über dort eingebundene Werbung auch von Werbevermarktern wie etwa Doubleclick. Beim Besuch einer weiteren Seite, die Werbung der Werbetreibenden enthält, kann über diese „Drittanbieter-Cookies“ erkannt werden, auf welchen Seiten Nutzer*innen zuvor waren. Wenn man die Cookies zusammennimmt, ergibt sich ein recht gutes Bild über die Interessen der Nutzer*innen.

Browserchronik

Ähnlich ist es mit der Chronik beziehungsweise der Verlaufsanzeige des Browsers. Wer darauf geachtet hat, dem ist möglicherweise aufgefallen, dass auf Websites benutzte Links die Farbe wechseln können und dass dies so geblieben ist, wenn die Website nach einiger Zeit erneut besucht wird. Die Information, was ein*e Nutzer*in sich beim letzten Besuch angesehen hat, wurde offenkundig gespeichert, konkret: in der Browserchronik. Diese Information kann aber von allen Seiten, die besucht werden, ausgewertet werden. Je länger eine Browserchronik zurückreicht, desto mehr verrät sie über die Nutzungsgewohnheiten der Surfer. Aus diesem Grund sollte sie hin und wieder gelöscht werden.

Datenspuren vermeiden

Vieles in Sachen Datenspuren hat man selbst in der Hand, insbesondere das, was man in sozialen Netzwerken und an anderen Stellen über sich preisgibt. Wie man sich und andere dort am besten schützen kann, was es zu beachten gilt und an wen man sich wenden kann, wenn man Unterstützung braucht, erfährt man auf den Seiten der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen.

Webseite der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen: www.ldi.nrw.de

Auch für Cookies und die Browserchronik kann man in den Einstellungen selbst festlegen, ob man diese erlaubt oder nicht oder dass diese Daten von Zeit zu Zeit automatisch gelöscht werden. Die meisten Browser bieten einen Privatmodus an, der dafür sorgt, dass solche Datenspuren vermieden werden. An anderen Stellen ist die Sache nicht so einfach, weil manches technisch bedingt ist. Aber auch hier lassen sich Datenspuren zumindest reduzieren. So gibt

Modul 2.3: Suchmaschinen

es datenschutzfreundliche Suchmaschinen wie Ixquick oder Startpage, die die IP-Adressen der Nutzer*innen anonymisieren oder gar nicht erst speichern.

6.4 Digitales Erbe

Immer mehr spielt sich unser Leben auch in der digitalen Welt ab, wir nutzen regelmäßig soziale Netzwerke, E-Mails oder Clouddienste. Dabei werden die digitalen Dienste nicht nur für die Kommunikation, sondern vermehrt auch für die Abwicklung von Einkäufen und sonstigen Geschäften genutzt. Alle, die längere Zeit das Internet genutzt haben, verfügen über eine hohe Anzahl an Benutzerkonten bei ganz unterschiedlichen Anbietern. Da fällt es schwer, den Überblick zu behalten. Hinzu kommen nicht selten digitale Güter, wie Filme, Spiele, Bücher, Musik, deren geldwerte Nutzungslizenzen ebenfalls an das Benutzerkonto gekoppelt sind.

Im Falle des Todes eines Menschen wollen oder müssen sich die Erben mit den digital gespeicherten Daten und Konten des oder der Angehörigen befassen. Diese geben nicht nur Auskunft über Kontakte, sondern zum Beispiel auch über offene Rechnungen oder laufende Verträge. Die zunehmende Digitalisierung sorgt Jahr für Jahr stärker dafür, dass wichtige Unterlagen, aber auch die Kommunikation mit Anbietern weniger in Papierform abgelegt werden, sondern stattdessen nur noch digital existieren. Da ist es wichtig, Vorsorge zu treffen, damit die Nachkommen und gewollten Erben auch den nötigen Zugriff erhalten.

Klare gesetzliche Regelungen, nach denen Erben einen Zugriff auf alle von einer verstorbenen Person angelegten Benutzerkonten erhalten, gibt es noch nicht (Stand 2020). Selbst die Frage, ob der digitale Nachlass überhaupt vererblich ist, ist rechtlich nicht eindeutig geklärt. Teilweise hat die Rechtsprechung mittlerweile digitale Dateien für vererbbar erklärt, andere Fragen bleiben hingegen noch offen. In zwei richtungsweisenden Urteilen aus den Jahren 2018 und 2020 hat der Bundesgerichtshof entschieden, dass die Plattform Facebook den Erben Zugang zum Nutzerkonto einer verstorbenen Person gewähren muss, da die Erben auch in die Rechtspositionen des oder der Verstorbenen in Bezug auf digitale Inhalte eingetreten sind. Ob sich dieses

Urteil jedoch verallgemeinernd auf alle digitalen Dienstleister beziehen lässt, ist rechtlich noch nicht abschließend geklärt. Eine gesetzgeberische Lösung, die klare Vorgaben macht, wäre sehr wünschenswert, sie lässt derzeit aber noch auf sich warten.

Tipp

Vertiefende Infos zum Nachlesen und Mustertexte finden sich unter: *https://s.rlp.de/Gc8rP*

Fehlt es Erben am Zugang zu den Konten, müssen sie daher mitunter selbst mit den jeweiligen Anbietern in Kontakt treten und den Erbfall und ihre Berechtigung mühsam nachweisen; ähnlich wie auch bei der Nachweispflicht für Aktien oder andere Wertanlagen wie Autos und Häuser. Ratsam ist deswegen, sich bereits zu Lebzeiten um den „digitalen Nachlass“ zu kümmern. Das heißt konkret, den Erben den Zugang zu den Vertragsbeziehungen zu Host-, Internet- oder E-Mail-Providern, aber auch zu Anbietern sozialer Netzwerke oder virtueller Konten zu sichern.

Digitales Erbe

Die folgenden Hinweise können den Erben den Zugriff auf das digitale Erbe erleichtern:

- Fertigen Sie eine Übersicht aller Nutzerkonten mit Benutzernamen und Kennwörtern an. Denken Sie dabei auch an alle kostenpflichtigen Abonnements und Mitgliedschaften, die nach Ihrem Tod gekündigt werden müssen.
- Sofern Sie einen Passwortmanager nutzen und dort alle Account-Zugänge hinterlegt sind, genügt es, den Zugang zum Passwortmanager zu verschaffen.
- Sie können die Übersicht ganz einfach analog als Liste auf Papier niederschreiben. Die Übersicht kann alternativ auch digital als verschlüsselte und kennwortgesicherte Datei gespeichert werden. Entweder man sichert diese auf dem PC/Laptop oder einem externen Medium wie einer ebenso gesicherten Festplatte oder einem USB-Stick. Daten auf Festplatten und USB-Sticks können jedoch verloren gehen, etwa wenn die Geräte aufgrund zu großen Alters defekt werden. Für welches Medium man sich auch entscheidet, wichtig ist es, die Liste an einem sicheren Ort zu deponieren, beispielsweise in einem Tresor oder einem Bankschließfach.

Digitales Erbe

- Bestimmen Sie eine Person Ihres Vertrauens zur Verwalterin oder zum Verwalter Ihres digitalen Nachlasses. Stellen Sie für diese Person eine Vollmacht aus, in der Sie festlegen, dass diese Person sich vollumfänglich und auch über Ihren Tod hinaus um Ihren digitalen Nachlass kümmern soll. Bei einigen Plattformen kann die Vertrauensperson in den Einstellungen schon zu Lebzeiten festgelegt werden.
- Regeln Sie in dieser Vollmacht genau, wie mit Ihrem digitalen Nachlass umgegangen werden soll. Welche Daten sollen gelöscht werden, was soll beispielsweise mit Fotos passieren, wie ist mit Ihrem Benutzerkonto in einem sozialen Netzwerk umzugehen? Bei dem sozialen Netzwerk Facebook ist es beispielsweise möglich, das Konto in einen Gedenkzustand zu versetzen.
- Legen Sie ebenfalls fest, was mit Ihren Endgeräten (Computer, Smartphone, Tablet) und den dort gespeicherten Daten passieren soll.
- Vergessen Sie nicht, die Vollmacht mit einem Datum zu versehen und zu unterschreiben.
- Übergeben Sie Ihrer Vertrauensperson die Vollmacht und informieren Sie Ihre Angehörigen darüber, dass Sie Ihren digitalen Nachlass auf diese Weise geregelt haben.
- Teilen Sie Ihrer Vertrauensperson ebenfalls mit, wo sie die Zugangsdaten zu Ihren Konten findet, also wo Sie zum Beispiel den USB-Stick deponiert haben.
- Denken Sie daran, die Auflistung Ihrer Accounts immer aktuell zu halten. Ergänzen Sie die Auflistung um neue Konten, löschen Sie die Daten in der Liste, wenn Sie sich bei einem Konto abgemeldet haben.
- Es gibt auch Firmen, die eine kommerzielle Nachlassverwaltung anbieten. Die Sicherheit solcher Unternehmen lässt sich allerdings nur schwer beurteilen.

6.5 Digitale Selbstverteidigung: Datenmissbrauch und Datensparsamkeit

Datenmissbrauch

Der sorgfältige Umgang mit den eigenen Daten im Internet ist nicht nur deshalb von Bedeutung, weil anderen Personen ein tiefer Einblick in die eigene Privatsphäre ermöglicht wird, sondern auch, weil persönliche Daten in den Fokus Krimineller geraten können. Anhand von zwei Beispielen soll deutlich gemacht werden, wie Identitätsdaten im Internet für kriminelle Machenschaften missbraucht werden können.

Phishing

Wie der Klang des englischen Wortes schon andeutet, geht es bei „Phishing“ im weitesten Sinne um das Thema „Fischen“, genauer gesagt um das Fischen nach Daten mit einem Köder. Als Köder schlüpft eine Person dabei in eine andere Identität, die einer Bank oder eines Onlineshops beispielsweise, mit dem Ziel, an sensible Daten der Nutzer*innen dieser Seiten zu gelangen. Dazu gehören Passwörter, PINs und TANs sowie Kunden- und Kreditkartennummern. Phishing-Attacken können sowohl per E-Mail als auch beim Besuch einer Internetseite erfolgen. Die Betrüger*innen fordern Nutzer*innen dazu auf, sich auf einer gefälschten Internetseite mit der persönlichen Kundennummer und dem Passwort anzumelden. Durch die Fälschung der Seite können sensible Daten abgegriffen, gesammelt und gespeichert werden. Häufig wird dabei das Design der echten Website oder E-Mails übernommen, sodass das Abgreifen der Zugangsdaten zumeist unbemerkt bleibt. Banken machen ihre Onlinebanking-Kund*innen immer wieder darauf aufmerksam, dass sie niemals per E-Mail die Angabe von Kontonummer, Passwort oder TANs verlangen würden.

Modul 7.1: E-Mailing

Modul 4.4: Sicheres Onlinebanking

Tipp

Mehr zum Thema „Wie erkenne ich eine Phishing-E-Mail?“ finden Sie hier: *https://s.rlp.de/RMunC*

Identitätsmissbrauch

Unter Identitätsmissbrauch versteht man die missbräuchliche Verwendung personenbezogener Daten durch Dritte. Name und Geburtsdatum einer Person reichen meist aus, um sich einer anderen Identität zu bemächtigen. Diese Daten finden sich in sozialen Netzwerken in großer Menge, und die Verwendung von Pseudonymen oder die Angabe falscher Daten wird von den Anbietern solcher Seiten häufig untersagt. Ziel des Identitätsmissbrauchs ist meist eine finanzielle Bereicherung, indem im Namen der oder des Betrogenen beispielsweise Geld abgehoben wird oder Einkäufe in Onlineshops getätigt werden. Auch um Straftaten zu begehen, werden Identitäten anderer Personen missbraucht.

Folgen von Identitätsmissbrauch: https://s.rlp.de/HJXr2

Modul 4.7: Passwörter und Schutz von mobilen Endgeräten

Neben Phishing sind es häufig Hackerangriffe auf die Anbieter, bei denen massenweise Daten von sozialen Plattformen, Onlineshops oder Kundenforen kopiert und gespeichert werden. Zumeist werden dabei Schwachstellen in den zentralen Systemen ausgenutzt. Das bedeutet, dass sich einzelne Nutzer*innen nicht wirklich dagegen schützen können, da nicht sie selbst, sondern die Anbieter im Fokus der Angreifer*innen stehen.

Tipp

Ob die eigenen Daten bereits Opfer eines Hacks wurden und möglicherweise im Internet kursieren, kann man beispielsweise mithilfe des „Identity Leak Checkers“ des Hasso-Plattner-Instituts unter *https://sec.hpi.de/ilc/* oder dem folgenden Link *https://haveibeenpwned.com/* herausfinden.

Datensparsamkeit

Der radikale Weg, zu verhindern, dass im Internet Daten über die eigene Person erhoben werden, wäre die Internetabstinenz. Dies kann und soll aber nicht die Lösung sein. Stattdessen gilt es, sich der bestehenden Risiken bewusst zu sein und stets abzuwägen, in welchem Verhältnis Kosten und Nutzen bei einzelnen Internetanwendungen stehen.

Das Ausfüllen von Onlineformularen

Kauft man online ein, müssen wahre Angaben gemacht werden, damit die Bestellung ankommt. Dennoch können auch hier Daten gespart werden: Oft müssen nicht alle Felder, die in dem Formular angegeben sind, auch wirklich ausgefüllt werden. Pflichtangaben sind meist mit einem kleinen Stern (*) gekennzeichnet. Dies gilt nicht nur beim Online-Einkauf, sondern auch für die Anmeldung bei einem E-Mail-Anbieter, in einem sozialen Netzwerk oder beim Ausfüllen eines Onlineformulars der Stadtverwaltung.

Lügen ausdrücklich erwünscht!

Bei manchen Angeboten ist es sinnvoll, ein Pseudonym zu nutzen. In Bezug auf E-Mails bietet es sich an, mehrere Adressen bei verschiedenen Anbietern anzulegen, um diese für unterschiedliche Zwecke zu nutzen. Wenn man sich der Seriosität eines Angebotes nicht sicher ist, kann man eine E-Mail-Adresse angeben, die keine Rückschlüsse auf die eigene Person zulässt (Beispiel: wolkenkratzer123@emailadresse.de). Für wenig sensible Zugänge (beispielsweise Foren), für die aber eine E-Mail-Adresse zur Registrierung unbedingt erforderlich ist, kommt auch die Nutzung einer sogenannten „Wegwerf-E-Mail-Adresse“ oder einer temporären E-Mail-Adresse in Betracht. Für die Registrierung bei sozialen Netzwerken oder E-Mail-Diensten werden in den Allgemeinen Geschäftsbedingungen oft „korrekte Angaben“ verlangt. Umso wichtiger ist, dass man sparsam mit den eigenen Daten umgeht und sich der Tragweite der Angaben bewusst ist. Äußerungen über politische und religiöse Einstellungen, das Hochladen von Fotos anderer Personen ohne deren Einverständnis oder das Diffamieren anderer Mitglieder sind auf den Seiten von sozialen Netzwerken tabu.

Identitätsmanagement

Das Internet und seine Dienste können auch gezielt genutzt werden, um das Onlineprofil nach den eigenen Wünschen zu gestalten. Dafür sollte man geschickt entscheiden, wo welche Daten preisgegeben werden. Wenn jemand sich als Expert*in in Sachen „Geschichte der Stadt Koblenz“ etablieren möchte, bietet es sich an, eine eigene Website zu dem Thema einzurichten oder sich mit Blogbeiträgen auf bestehenden Websites zu beteiligen. Ebenso kann man eigene Dokumente zum jeweiligen Thema online stellen oder sich in sozialen Netzwerken mit Gleichgesinnten vernetzen.

Grundsätzliche Tipps zum Umgang mit Daten

„Informierte Einwilligung“: Prinzipiell kann ein Internetanbieter Daten von Personen auf zulässiger Basis speichern, verwenden und weitergeben, wenn die jeweilige Person zuvor ausreichend unterrichtet wurde und zugestimmt hat. Diesen Umstand nennt man „informierte Einwilligung“. Deshalb empfiehlt sich das Lesen der Allgemeinen

Geschäftsbedingungen und der Datenschutzerklärung, bevor man diesen per Klick zustimmt. Dort sollten auch Hinweise zu finden sein, wie man die Einwilligung widerruft oder sich beispielsweise von einem Newsletter abmeldet, auch wenn es bei bestehenden Einwilligungserklärungen oft an Transparenz oder Auswahlmöglichkeiten mangelt.

Nutzung eines „zweiten Faktors“: Möchte man sich bei einer Seite registrieren, so ist zumindest die Kombination aus Benutzername und Passwort notwendig, um sicherzustellen, dass sich Unberechtigte nicht einfach anmelden und den Zugang missbrauchen können. Insbesondere beim Zugang zum Onlinebanking ist heutzutage ein sogenannter zweiter Faktor zumeist verpflichtend. Das bedeutet, dass man nicht nur den Benutzernamen und das Passwort („erster Faktor“) benötigt, um sich zu einem Dienst anzumelden, sondern noch einen zusätzlichen Code. Dieser wird zufällig erzeugt („zweiter Faktor“) und beispielweise per SMS oder über eine besondere App zugestellt. Da dieser Code jedes Mal erneut zufällig erzeugt wird und nur über ein persönliches Endgerät, zum Beispiel ein Handy, zugestellt wird, sinkt das Missbrauchsrisiko um ein Vielfaches. Sofern ein Dienst also die Möglichkeit einer „Zwei-Faktor-Authentifizierung“ (so der Fachbegriff) bietet, sollte diese genutzt werden.

Modul 4.7:
Passwörter und Schutz von mobilen Endgeräten

Cookie-Banner: Ein sogenanntes Cookie-Banner ist eine Art Interaktion, die beim ersten Besuch einer Website zwischen den Besucher*innen und der Seite stattfindet. Es geht dabei um die durch die Website verarbeiteten Daten und deren Nutzung durch den Betreiber. Auch wenn sie zumeist als lästig empfunden werden, sind Cookie-Banner – insofern sie korrekt umgesetzt werden – eine nützliche Sache. So kann man hierüber etwa steuern, dass die eigenen Daten nicht zur Profilbildung genutzt oder an Dritte zu Werbezwecken weitergegeben werden. Hiervon sollte man immer zu eigenen Gunsten Gebrauch machen, auch wenn diese Dialoge manchmal gar nicht so einfach zu verstehen sind beziehungsweise die gewünschte Ablehnung etwas versteckt ist. Hartnäckigkeit wird belohnt! Wer Websites die Cookies verpflichtend vorschreiben, dennoch nutzen will, auch wenn das Cookie-Tracking möglichst unterbunden werden soll, kann im Browser einstellen, dass Cookies nach jeder Sitzung gelöscht werden sollen.

Noch weiter gehend ist der sogenannte private Modus, der generell jedweder Seite das Setzen von Cookies untersagt.

Modul 2:
Wie man das
Internet nutzt

Werbeblocker: Viele Webseiten sammeln auch Daten über ihre Nutzer*innen, die diese nicht explizit eingeben, sondern die durch die bloße Benutzung der Seite entstehen, etwa beim „Bummeln“ auf der Website eines Onlineshops. Auf diese Art werden sogenannte Nutzerprofile erstellt, die letztendlich dazu dienen, den jeweiligen Nutzer*innen möglichst attraktive Werbung anzuzeigen. Hiergegen können sogenannte Werbeblocker helfen. Diese sind entweder bereits Bestandteil moderner Browser oder können diesen ergänzend hinzugefügt werden. Die Besonderheit: Sie sorgen nicht nur dafür, dass weniger bis gar keine Werbung mehr angezeigt wird. Sie erschweren den Seitenbetreibern zumeist auch die Erstellung von Nutzerprofilen.

Regelmäßig Inventur machen: Nach vielen Jahren der Internetnutzung sammeln sich erfahrungsgemäß Zugangsdaten zu zahlreichen Websites an, seien es Online-Apotheken, Foren oder soziale Netzwerke. Gerade bei Onlineshops kommt es vor, dass dieser nur für eine einzige Bestellung genutzt wurde, etwa, weil das gesuchte Produkt dort gerade am günstigsten war. Neben den Bestellungen sind dort in der Regel die echten Adressdaten sowie häufig auch Bankdaten hinterlegt. Sofern man den Dienst längere Zeit nicht genutzt hat oder eine künftige Nutzung gleich ausschließt, sollte das Benutzerkonto dort gekündigt und auf die Löschung der Daten bestanden werden. So werden die Daten nicht zum Ziel potenzieller Angreifer*innen der Anbieter. Die Kündigung erfolgt am besten schriftlich.

Tipp

Bei vielen Onlineshops kann man alternativ zur Registrierung auch als Gast bestellen. Das heißt, man gibt die benötigten Informationen nur zur Durchführung genau einer Bestellung an und muss sich nicht registrieren und dadurch weitere (Zugangs-) Informationen hinterlegen.

Seien Sie misstrauisch: Anonymität im Netz kann eine Chance sein. Aber es gibt auch Internetnutzer*innen, die die Möglichkeiten des anonymen Surfens ausnutzen. Deswegen ist Vorsicht geboten. Die Verwendung von sicheren Passwörtern, hohe Sicherheitseinstellungen und das Surfen auf seriösen Internetseiten wird empfohlen. Nutzen Sie die Möglichkeit einer „Zwei-Faktor-Authentifizierung".

Kennen Sie Ihre Rechte: Jede*r Betroffene hat das Recht auf Auskunft, Berichtigung, Einschränkung und Löschung, wenn es um die Verarbeitung der persönlichen Daten geht. Außerdem dürfen die Daten grundsätzlich nur für genau den Zweck verwendet werden, für den sie erhoben wurden. Nutzer*innen müssen einer Verarbeitung oder Nutzung der Daten etwa zu Werbezwecken oder im Rahmen der Markt- und Meinungsforschung in der Regel ausdrücklich zustimmen. Diesen Vorgang nennt man „Einwilligung". Einer erteilten Einwilligung kann auch widersprochen werden, was eine Löschung der Daten zur Folge hat.

Wenn man also beispielsweise wissen möchte, welche Daten ein Unternehmen über die eigene Person gespeichert hat, kann man darüber Auskunft erhalten. Hierzu wendet man sich an die oder den in der Datenschutzerklärung angegebenen Datenschutzbeauftragte*n der Verantwortlichen. Auf dem gleichen Weg kann man auch eine Löschung oder Berichtigung der Daten fordern. Die Verantwortlichen müssen solche Anfragen zeitnah und fristgerecht bearbeiten.

Weitere Informationen zu Ihren Rechten: https://s.rlp.de/mBpuu

Musterbrief Erfragung der Daten: https://s.rlp.de/OuoDd

6.6 Das Recht am eigenen Bild

Gerade auf sozialen Plattformen spielt das Einstellen von Fotos eine große Rolle. Stellt man Fotos auf die eigene Website oder macht Fotoalben im Netz für einen bestimmten Personenkreis zugänglich, sollte man das sogenannte Recht am eigenen Bild kennen und beachten.

Grundsätzlich gilt, dass Abbildungen, also auch Fotos oder Videos, nur mit Einwilligung der abgebildeten Personen verbreitet oder öffentlich zur Schau gestellt werden dürfen. Abbildungen beziehungsweise Bildnisse im Sinne des sogenannten Kunsturhebergesetzes sind übrigens nicht nur Fotografien, sondern jede erkennbare Wiedergabe des äußeren Erscheinungsbildes einer Person, also auch in Zeichnungen oder Karikaturen.

Hat man keine Einwilligung der abgebildeten Person, so reicht es häufig nicht, diese Person durch die in Presseveröffentlichungen üblichen Augenbalken unkenntlich zu machen, denn häufig ist sie bereits durch den Kontext oder durch andere Merkmale identifizierbar. Die Erkennbarkeit einer Person entfällt auch dann nicht, wenn sie sich altersbedingt verändert hat. Eine Veröffentlichung ohne Einwilligung ist erst zulässig, wenn eine Identifizierung der Person nicht mehr möglich ist. Eines Beweises, dass die Person tatsächlich erkannt wird, bedarf es nicht.

6.7 Fotografieren erlaubt?

In aller Regel darf eine Privatperson für den eigenen familiären oder persönlichen Gebrauch immer Fotos machen. Es gibt jedoch ein paar Ausnahmen, die auch durch das Strafgesetzbuch geregelt werden. Das Fotografieren ist in folgenden Fällen nicht erlaubt:

Strafgesetzbuch § 201a StGB

- bei unbefugt angefertigten Bildern von einer anderen Person, die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet (z. B. Umkleidekabinen, Toiletten),
- bei unbefugt angefertigten Bildern, die die Hilflosigkeit einer anderen Person zur Schau stellen,
- bei Bildaufnahmen, die die Nacktheit einer anderen Person unter 18 Jahren zum Gegenstand haben und mit dem Ziel hergestellt wurden, sie einer dritten Person gegen Entgelt zu verschaffen oder anzubieten.

Auch im privaten Kontext ist jedoch stets der Wille der abgebildeten Personen zu berücksichtigen: Wünscht eine Person, nicht fotografiert zu werden, darf kein Foto gemacht werden oder ein gemachtes Bild muss gelöscht werden. Die betroffene Person muss für ihre Entscheidung keine Gründe nennen, denn das Recht am eigenen Bild gibt jedem Menschen genau diese Entscheidungsfreiheit, selbst zu entscheiden, wer, wann und in welcher Situation ein Foto von ihm macht.

Einwilligung

Wer Fotos veröffentlichen möchte, auf denen Personen zu sehen sind, braucht grundsätzlich deren Einwilligung. Werden Minderjährige abgebildet, so müssen alle Sorgerechtsberechtigten einwilligen, solange der oder die Jugendliche noch nicht einsichtsfähig ist. In der Regel sind Jugendliche ab 16 Jahren einwilligungsfähig.

Keine Einwilligung benötigt man nach dem sogenannten Kunsturhebergesetz, wenn einer der folgenden Punkte zutrifft:

- Es handelt sich um ein Bildnis der Zeitgeschichte. Ein Bildnis der Zeitgeschichte liegt etwa bei Besuchen von Politikern oder berühmten Personen vor. Die Ausnahme umfasst jedoch auch weitere Konstellationen: Ein Bildnis aus dem Bereich der Zeitgeschichte kann nicht nur Vorgänge von historischer oder politischer Bedeutung, sondern ganz allgemein das Zeitgeschehen unter Berücksichtigung sämtlicher sozialer, wirtschaftlicher und kultureller Aspekte, somit alle Fragen von allgemeinem gesellschaftlichen Interesse des Kulturlebens, der Wirtschaft und des Sports, eingeschlossen Unfälle, Verbrechen, Kriegshandlungen oder Naturkatastrophen zeigen.

- Bilder, auf denen Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeiten erscheinen. Bei diesen Bildern ist das Hauptmotiv des Bildes die Landschaft beziehungsweise die allgemeine Umgebung und nicht die Person auf dem Bild. Dabei darf die Abbildung der Person nicht im Vordergrund stehen. Die Person darf sich also nur zufällig in einer Umgebung befinden. Beispiel: ein Foto des Mainzer Doms, auf dem am Rand auch Tourist*innen abgebildet sind.

- Bilder von öffentlichen Veranstaltungen, Aufzügen und ähnlichen Vorgängen (zum Beispiel Demonstrationen, Sportveranstaltungen, politische Versammlungen oder Paraden). Die Veranstaltungen müssen in der Öffentlichkeit stattfinden und die Abgebildeten müssen einen kollektiven Willen besitzen, gemeinsam an dieser Veranstaltung teilzunehmen. Der zufällig zusammenbefindlichen Gruppe von sonnenbadenden Parkbesucher*innen oder wartenden Fahrgästen an der Bushaltestelle fehlt es an diesem kollektiven Willen, sodass Bilder von diesen Gruppen nicht ohne eine Einwilligung veröffentlich werden dürfen.

Wie kann eine Einwilligung erteilt werden?

Die Einwilligungserklärung muss nicht zwingend schriftlich erfolgen. Will ein*e Fotograf*in später jedoch einen Beweis haben, dass abgebildete Personen in die Veröffentlichung eingewilligt haben, empfiehlt es sich, um eine schriftliche Einwilligung zu bitten.

Die Einwilligung kann auch durch schlüssiges Verhalten erfolgen, sofern damit eine aktive bestätigende Handlung verbunden ist. Allein die Anwesenheit der abgebildeten Person zum Zeitpunkt einer Aufnahme oder das Betreten einer Veranstaltung, bei der Fotoaufnahmen erstellt werden sollen, reichen zum Beispiel nicht für eine Einwilligung aus. Das aktive Hinzutreten zum Zweck einer Aufnahme kann jedoch als Einwilligung in das Anfertigen des Fotos gewertet werden. Dieses schlüssige Verhalten kann jedoch nur dann eine Einwilligung zur Veröffentlichung des Bildes sein, wenn die betroffene Person vorher über die Veröffentlichungsabsicht und die Form der Veröffentlichung informiert wurde.

Die abgebildete Person hat jederzeit die Möglichkeit, ihre Einwilligung zu widerrufen. In diesem Fall darf das Bild nicht (mehr) veröffentlicht werden.

Was kann man tun?

Was mit einmal gemachten Fotos passiert, können die Abgebildeten beeinflussen, denn ohne deren Einwilligung ist es grundsätzlich nicht zulässig, Fotos zu verbreiten. Dies gilt auch für das private Umfeld. Die öffentliche Zurschaustellung, somit auch die Veröffentlichung im Internet, ist ohne Einverständnis nicht zulässig.

Wird das Recht am eigenen Bild verletzt, kann von der abgelichteten Person Strafanzeige erstattet werden. Außerdem hat sie Anspruch auf Unterlassung, um die Erstveröffentlichung des Bildes oder eine wiederholte Veröffentlichung zu verhindern. Auch ein Anspruch auf Schadensersatz kann unter Umständen in Betracht kommen. Wurden die Fotografien unbefugt erstellt, darf man die Herausgabe oder Vernichtung der Negative und aller Abzüge verlangen. Außerdem hat man Anspruch darauf, zu erfahren, inwieweit und wohin die Bilder weitergegeben wurden. Allerdings ist die Verbreitung von Bildern im Internet nur schwer nachzuvollziehen.

Die große Herausforderung ist es, einerseits die Freiheit und Verfügbarkeit des Internets zu wahren, andererseits aber auch die Rechte der Nutzer*innen zu stärken.

INTERVIEW MIT

Roul Tiaden

Ständiger Vertreter der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen

Wie steht es um Datenschutz und den Schutz der Privatsphäre in der digitalen Welt? Wo sehen Sie besondere Herausforderungen für NRW?

Roul Tiaden: Das Internet bietet mit seinem stets global verfügbaren, effizienten Zugang zu Informationen und den nahezu unbegrenzten Möglichkeiten zum sozialen Austausch viele Freiheiten und Vorteile. Gerade was das Thema Datenschutz und Schutz der Privatsphäre betrifft, birgt es aber auch zahlreiche Risiken. So ist es im Alltag der meisten von uns oft gar nicht so einfach, personenbezogene Daten zu schützen. Allein das Surfen im Internet kann dazu führen, dass aus personenbezogenen Nutzungsdaten, wie der IP-Adresse oder dem Besuch bestimmter Websites, Nutzungsprofile erstellt werden. Unternehmen wie Google, Facebook & Co. können solche Daten verwenden, um z. B. verhaltensbasierte Werbung gewinnbringend zu adressieren. Die große Herausforderung ist es, einerseits die Freiheit und Verfügbarkeit des Internets zu wahren, andererseits aber auch die Rechte der Nutzer*innen zu stärken. Daher müssen die Unternehmen zur Verantwortung gezogen werden, die für die Verarbeitung personenbezogener Daten eine Rechtsgrundlage brauchen und z. B. individuelle Konfigurationsmöglichkeiten und transparente Nutzungsbedingungen schaffen müssen. Zugleich müssen die Nutzer*innen für die Risiken und Gefahren sensibilisiert werden.

Im Internet werden Unmengen von Daten erhoben und verarbeitet – zu welchen Zwecken?

Roul Tiaden: Die Website-Betreiber selbst geben häufig als Zweck für die Verarbeitung der personenbezogenen Nutzerdaten ihr „berechtigtes Interesse" an, welches zumeist ein wirtschaftliches ist: Nutzerdaten werden gesammelt und ausgewertet, um z. B. die Angebote besser an die Nutzer*innen (als potentielle Kund*innen) auszurichten oder passende Werbung auszuspielen. Diese wirtschaftlichen Interessen sind durchaus legitim. Die DS-GVO sieht jedoch vor, dass auch die Interessen der Nutzer*innen zu berücksichtigen sind. Das bedeutet, dass zwischen den unterschiedlichen Interessen abgewogen werden muss. Nutzer*innen rechnen z. B. in der Regel nicht damit, dass ihre Daten ohne ihr Wissen und ohne ihren Einfluss an andere Unternehmen für deren Zwecke weitergegeben werden. Diese Art von Tracking darf daher nicht ohne informierte, vorherige Einwilligung der Nutzer*innen erfolgen.

Wo wünschen Sie sich mehr Vorsicht von den Nutzer*innen?

Roul Tiaden: Eine große Gefahr stellen Schadprogramme dar. Diese können Daten nicht nur vernichten, sondern auch Informationen an Kriminelle übermitteln. Anschließend wird mit der Veröffentlichung der Daten gedroht, die nur durch die Zahlung einer bestimmten Summe „Lösegeld" abgewendet werden könne. Auch ein anderweitiger Missbrauch der so erlangten Daten kann nicht ausgeschlossen werden.

Internetnutzer*innen sollten sich bewusstmachen, dass sie nicht anonym im Netz unterwegs sind, sondern Datenspuren hinterlassen. Daten sollten möglichst kontrolliert veröffentlicht oder weitergegeben werden. Dies gilt sowohl in sozialen Netzwerken und Foren, als auch z. B. beim Ausfüllen von Formularen oder beim Online-Shopping. Gerade bei Gewinnspielen steht bei unseriösen Anbietern im Vordergrund, an Nutzerdaten zu kommen, um sie für Telefon- oder E-Mail-Werbung zu nutzen.

Nutzen Sie selbst als Datenschutzexperte bedenkenlos digitale Angebote, z. B. Smartphone-Apps?

Roul Tiaden: Selbstverständlich nutze auch ich das Internet, das für mich vor allem eine wichtige Informationsquelle darstellt. Ich schütze meine Privatsphäre jedoch, indem ich auf meinen Geräten datenschutzfreundliche Voreinstellungen verwende. Auf besonders datenhungrige Apps verzichte ich.

Glossar

Account: Ein Account ist ein Benutzerkonto für einen Onlinedienst, zum Beispiel für einen E-Mail-Service oder eine Videoplattform. Meistens gewährt dieses Benutzerkonto Zugang zu gespeicherten persönlichen Informationen oder zu sonst nicht frei zugänglichen Bereichen einer Internetseite oder eines Internetdienstes.

Algorithmus: Algorithmen sind komplexe mathematische Formeln, die miteinander verknüpft sind und im Ergebnis eine Kette von Regeln oder Anweisungen bilden, die zum Beispiel Grundlage einer computergesteuerten Entscheidung sein können.

Anonymität: Anonymität ist ein Zustand, in dem Daten über eine bestimmte Person eben dieser Person nicht zugeordnet werden können, da die zugehörigen Identifikationsdaten wie Name, Anschrift, Ausweisnummer etc. fehlen.

analog und digital: Bei der analogen und der digitalen Signalübertragung geht es zunächst um die Frage, wie ein Signal von einem Sender zu einem Empfänger kommt. Ein Beispiel hierfür ist die Übertragung von Musik etwa einer Schallplatte oder einer CD zu einem Verstärker. Bei einer klassischen Schallplatte wird die Musik analog in Form eines elektrischen Signals übertragen. Der Begriff „analog“ kommt aus dem Griechischen und bedeutet „ähnlich“. Analoge Signale ähneln dem, was sie wiedergeben. Eine Schallplatte gibt Tonschwingungen wieder und erzeugt daraus eine elektrische Schwingung. Diese Schwingung nimmt dabei viele unterschiedliche Spannungswerte an. Bei der digitalen Übertragung, beispielsweise bei der Aufnahme einer CD, werden Tonschwingungen in eine eigene digitale Sprache übersetzt.

Im Vergleich zum analogen Signal gibt es beim digitalen nur zwei Spannungen oder zwei Werte. Man nennt dies auch „binäre Codierung“ (1 oder 0). Die Kunst beim Digitalen besteht darin, analoge Signale aus der Umwelt (Stimmen, Töne etc.) in digitale zu übersetzen. Der Vorteil ist die universelle Einsatzmöglichkeit: Sind sie einmal digital, können Daten nahezu überall in der digitalen Welt eingesetzt werden, beispielsweise weil die Tonaufnahme in Form von Daten vorliegt. Eine CD kann im Computer gelesen und die Musikstücke auf den PC

kopiert werden. Von dort kann die Musik mithilfe von Programmen in eine MP3-Datei umgewandelt und auf den MP3-Player übertragen werden und so weiter. Eine Schallplatte hingegen kann nur von einem Schallplattenspieler gelesen werden und ist daher nicht universell nutzbar.

Ein weiterer Vorteil des Digitalen ist die Möglichkeit, unterschiedliche Inhalte miteinander zu kombinieren, wie Audio, Video und Text. Dies geht nur, weil beim Digitalen eine Art Universalsprache zum Einsatz kommt. Dieser verdanken wir auch, dass zum Beispiel der Computer alle möglichen Inhalte wiedergeben und kombinieren kann.

App: Die Abkürzung „App" steht für das englische Wort „**App**lication", was so viel wie „Anwendung" bedeutet. Diese Anwendungen sind nichts anderes als Programme, die je nach Funktionalität mal größer und mal kleiner im Datenumfang sind. Der Begriff „Apps" ist in seiner Verwendung sehr eng an Smartphones und Tablet-Computer gebunden. Apps bezieht man über spezielle Stores (virtuelle Einkaufsläden), am sichersten über den Anbieter des geräteeigenen Betriebssystems.

Benutzerkonto: siehe *Account*

Betriebssystem: Das Betriebssystem ist die Schaltzentrale eines PCs, Smartphones oder Tablets. Es verwaltetet alle verbauten Komponenten wie Festplatten, Grafikkarten oder Arbeitsspeicher und stellt den Nutzer*innen eine grafische Oberfläche zur Verfügung, mit der sowohl Programme aufgerufen als auch Dateien verwaltet werden können. Bekannte Betriebssysteme für PCs sind Windows, macOS oder Linux, für mobile Geräte Android und iOS. Damit keine Schädlinge auf einen Computer gelangen und Sicherheitslücken seitens Krimineller genutzt werden können, ist es wichtig, das Betriebssystem immer auf dem aktuellen Stand zu halten und regelmäßig Aktualisierungen, sogenannte Updates, vorzunehmen.

Browser: Egal ob am Laptop oder Smartphone: Browser sind der Dreh- und Angelpunkt des Internetgebrauchs. Das Wort „Browser" kommt aus dem Englischen, das Verb „to browse" bedeutet „durchstöbern". Browser machen das Anschauen von Internetseiten im

World Wide Web erst möglich. Sie können den sogenannten Quelltext, der auf Websites hinterlegt ist, lesen und ihn grafisch darstellen. Bekannte Browser sind Microsoft Edge, der bereits auf den meisten Computern mit Windows als Betriebssystem installiert ist, Mozilla Firefox und Google Chrome, die oft separat installiert werden müssen. Auf Smartphones mit Android als Betriebssystem ist Google Chrome häufig standardmäßig als Browser eingerichtet. Der Standardbrowser für Apple-Geräte ist Safari.

Cookies: Kekse und Plätzchen werden im Englischen „Cookies" genannt. Nun hat der Cookie im Laptop, Smartphone oder Tablet aber nichts mit dem süßen Gebäck zu tun. Cookies sind vielmehr „Krümel" in Form kleiner Textdateien, die dazu genutzt werden, auf einem Computer persönliche Daten oder Einstellungen von Nutzer*innen zu hinterlegen. Onlineshops oder soziale Netzwerke nutzen diese Datenspuren beispielsweise, um ihre Angebote auf die jeweiligen Besucher*innen zu personalisieren.

Datenpaket: Unter einem Datenpaket versteht man, vereinfacht gesagt, einen Teil eines Datenstroms, also eine konkrete Dateneinheit, die beispielsweise über das Internet versendet wird. Im Gegensatz zum Datenstrom hat das Datenpaket eine definierte Größe und Form, die sich zum Beispiel in der Kommunikation zwischen zwei Computern auf Vollständigkeit überprüfen lässt.

digital: siehe *analog und digital*

Hacker: Als Hacker werden Personen bezeichnet, welche widerrechtlich digitale Sicherheitsbarrieren umgehen und sich so Zugriff auf ein Computersystem verschaffen. Dadurch können elektronisch gespeicherte oder versendete Daten abgegriffen werden und sind dann unberechtigten Dritten zugänglich. Die Durchführung einer solchen Handlung wird als „hacken" bezeichnet.

Handy: Der Begriff „Handy" hat sich in Deutschland als Synonym für die Begriffe „Mobiltelefon" beziehungsweise „Smartphone" durchgesetzt. Handy ist nur eine scheinbare Entlehnung, denn im Englischen bedeutet das Wort so viel wie „handlich, geschickt". Im englischen

Sprachraum werden für Mobiltelefone eher die Begriffe „mobile (phone)“ oder „cell(ullar) phone“ genutzt.

Internet: Das Internet ist ein weltweit zwischenverbundenes Computernetzwerk (auf Englisch „**Inter**connected **Net**work“). Das bedeutet, dass viele einzelne Netzwerke, zum Beispiel von Firmen, öffentlichen Einrichtungen oder auch privaten Nutzer*innen, in einem Netzwerkverbund stehen.

IP-Adresse: „**I**nternet-**P**rotocol“-Adressen sind die digitalen Fingerabdrücke im Netz. Jeder PC im Internet erhält seine eigene, nur einmal vorhandene IP-Adresse. Vergleichbar ist diese mit der Postanschrift. Nur können mit IP-Adressen Computer untereinander Daten austauschen und Informationen hin- und herschicken.

LAN: Die Abkürzung „LAN“ steht für den englischen Begriff „**L**ocal **A**rea **N**etwork“ (zu Deutsch „lokales Netzwerk“). Router und PC sind über ein Kabel miteinander verbunden. Ist dies nicht der Fall, ist das Netzwerk also kabellos (englisch „wireless“), nennt man es „Wireless Local Area Network“, abgekürzt „WLAN“.

Link: Der Begriff „Link“ leitet sich ab vom englischen Verb „to link“, was „verbinden“ bedeutet. Unter einem Link versteht man einen digitalen (Quer-)Verweis auf eine andere Stelle innerhalb einer Website, auf eine externe Internetseite, auf eine Datei oder eine Anwendung innerhalb des Internets. Links sind deshalb auch zentrale Strukturelemente des Internets.

Newsletter: Newsletter sind Mitteilungsblätter im Internet, wie zum Beispiel Informations-E-Mails über Organisationen, Initiativen oder neue Angebote, die meist abonniert werden müssen (und auch wieder abbestellt werden können). Newsletter werden meistens in regelmäßigen Abständen verschickt und informieren über Neuigkeiten wie Angebote, Veranstaltungen oder Nachrichten.

Passwort: Passwörter sind Losungswörter, mit denen der Zugang zu einem bestimmten Bereich im Internet gewährt wird. E-Mail-Konten, Onlinebanking und viele andere Benutzerkonten werden in der Regel

mit einem Passwort versehen, damit nicht jede*r darauf zugreifen kann. Passwörter sollten mindestens acht Stellen haben und aus Buchstaben, Sonderzeichen sowie Ziffern bestehen.

personenbezogene Daten: Alle Daten, die sich direkt mit einer Person in Verbindung bringen lassen, nennt man personenbezogene Daten. Solche Daten können zum Beispiel der volle Name in Kombination mit der Adresse, der Telefonnummer und den Bankdaten sein. Personenbezogene Daten sind sehr sensible Daten, da sie tiefe Einblicke in die Privatsphäre eines Menschen erlauben.

Phishing: Beim Phishing geht es darum, mit gefälschten E-Mails und anderen Nachrichtenformen an Daten von Nutzer*innen zu kommen. Dabei werden Nutzer*innen auf gefälschte Websites gelockt, um dort ihre Daten preiszugeben. Beispielsweise erhält man eine E-Mail, in der man dazu aufgefordert wird, die eigenen Bankdaten auf einer Website anzugeben. Die entsprechende Seite sieht der Originalseite der Bank sehr ähnlich, ist allerdings eine Betrugsseite. Der Begriff „Phishing“ setzt sich zusammen aus den Wörtern „fishing“ (zu Deutsch „angeln“) und „Passwort“. Phishing ist also das Angeln nach Passwörtern.

PIN: Als „**P**ersönliche **I**dentifikations**n**ummer“ wird eine meist vierstellige Ziffernfolge bezeichnet, mit der man sich bei einem Gerät authentisieren kann. PINs werden vor allem zum (Ent-)Sperren von Smartphones sowie in Verbindung mit Bankkarten verwendet.

Profil: Profile im Internet sind vergleichbar mit einem Steckbrief. Sie dienen dazu, Informationen über einzelne Nutzer*innen anzuzeigen. In sozialen Netzwerken können Profile selbst angelegt und bearbeitet werden. In anderen Anwendungen wie Personensuchmaschinen werden von der Suchmaschine selbst Profile von Nutzer*innen angelegt, die aus Daten gewonnen werden, die bereits im Internet zu finden sind.

Provider: Als „Provider“ bezeichnet man den Dienstanbieter für den Internetzugang. Dieser ist häufig zugleich der Telefonanbieter.

Server: Wie die Bezeichnung „Server“ (zu Deutsch „Diener“ oder „Zusteller“) schon andeutet, liegt die Funktion eines Servers in der Bereitstellung von Daten oder Anwendungen für die Teilnehmer*innen eines Netzwerks wie dem Internet. Dabei kann es sich bei einem Server entweder um einen Computer selbst oder auch nur um ein Programm handeln.

Smartphone: Der auch im deutschen Sprachraum genutzte Begriff „Smartphone“ bedeutet „intelligentes oder geschicktes Telefon“. Die Funktionalität von Smartphones geht dabei weit über die eines reinen Telefons hinaus. Smartphones sind Minicomputer, die die Nutzung von vielen Programmen wie Kalender, E-Mail oder anderen Internetdiensten ermöglichen. Besondere Merkmale der Smartphones sind hochauflösende Displays (Anzeigen), zahlreiche Sensoren wie GPS und die Bedienung über Touchscreen.

Tablet: Ein Tablet ist ein internetfähiges Gerät, dessen Größe zwischen Smartphone und Laptop liegt. Der englische Begriff „Tablet“ meint im Deutschen einen „Schreibblock“ oder eine „kleine Tafel“. Für den tragbaren Computer haben sich im deutschen Sprachgebrauch aber auch die Begriffe „Tablet-Computer“ und „Tablet-PC“ durchgesetzt. Im Vergleich zu Smartphones haben Tablets oft keinen SIM-Karten-Slot und sind damit auf eine WLAN-Verbindung angewiesen, um ins Internet zu gehen. Wer ein Tablet auch mobil nutzen möchte, der sollte darauf achten, ein Gerät mit einem SIM-Karten-Slot für den Zugang zum Mobilfunknetz zu kaufen.

TAN: Die Abkürzung „TAN“ steht für „**T**rans**a**ktions**n**ummer“. Diese Nummer ist eine Art Einmalpasswort und findet meist im Onlinebanking Anwendung.

Unterlassung: Mit dem Unterlassungsanspruch kann eine künftige Beeinträchtigung oder drohende Störung rechtlich abgewehrt werden.

Update: Bei einem Update wird ein Programm auf den aktuellen Stand gebracht. Hierfür muss in den meisten Fällen das Programm selbst mittels einer Internetverbindung auf einen Rechner der Herstellerfirma zugreifen können, um dort die Version des Programms auf dem

heimischen Computer mit der auf dem Computer des Herstellers abzugleichen und gegebenenfalls zu aktualisieren. Updates sollten regelmäßig vorgenommen werden.

WLAN: siehe *LAN*

Zwei-Faktor-Authentifizierung: Damit ist gemeint, dass der Zugriff zu einem bestimmten Dienst erst gewährt wird, wenn die Berechtigung des Nutzers oder der Nutzerin durch zwei voneinander unabhängige Identifikationsmethoden geprüft wurde. In der Regel können die Methoden aus folgenden Bereichen ausgewählt werden: Wissen (Passwort oder Code), Gerät (Chip-Lesegerät oder Smartphone) und biometrische Kennung (Fingerabdruck, Gesichts- oder Retinascan).

Autor*innen

Helmut Eiermann ist der stellvertretende Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz und leitet dort den Bereich Querschnittsaufgaben. Er kümmert sich um Fragen des technischen Datenschutzes und der Datensicherheit. Vor seiner Tätigkeit für den Datenschutzbeauftragten war er in der Bundesverwaltung tätig.

Dr. Julia Gerhards arbeitet bei der Verbraucherzentrale Rheinland-Pfalz als Referentin für Verbraucherrecht und Datenschutz. Neben Aufklärung und Information der Verbraucher zu diesen Themen gehört vor allem die politische Interessenvertretung zu ihren Aufgaben. Die Nutzbarkeit digitaler Möglichkeiten bei gleichzeitigem Schutz der Privatsphäre ist dabei eines ihrer Anliegen.

Timo Göth* ist Mitarbeiter beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz im Bereich Technik. Zu seinen Aufgaben gehören unter anderem die Kontrolle und Beratung in Fragen des technischen Datenschutzes und der Datensicherheit. Vor seiner Arbeit für den Datenschutzbeauftragten war der Diplom-Informatiker (FH) im Hochschulbereich tätig.

Maximilian Heitkämper leitet den Fachbereich Digitales und Verbraucherrecht bei der Verbraucherzentrale Rheinland-Pfalz. Bereits im juristischen Studium waren Digitalisierung und wettbewerbsrechtliche Themen sein inhaltlicher Fokus. Zunächst als Rechtsreferent im Projekt Marktwächter Digitale Welt angestellt, übernahm er 2019 schließlich den neu geschaffenen Fachbereich.

Sonja Wirtz* arbeitet als Referentin beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz. Sie betreut den Bereich Medien sowie das Referat Leben im Bereich Wirtschaft. Zu ihren Aufgaben gehören u.a. die Kontrolle und Beratung in Fragen des Verbraucherschutzes. Daneben betreut sie Beschwerdeverfahren gegen die Wohnungswirtschaft, Vereine sowie Parteien.

**Frau Wirtz und Herr Göth verzichten auf die Abbildung ihrer Portraits. Als Mitarbeiter des Datenschutzbeauftragten des Landes Rheinland-Pfalz ist ihnen das Recht am eigenen Bild sehr wichtig und sie machen hier Gebrauch von diesem.*

Impressum

Titel:
Smart Surfer – Fit im digitalen Alltag
Lernhilfe für aktive Onliner*innen

Projektkoordination:
Verbraucherzentrale Rheinland-Pfalz e.V.
Laura Günther
Seppel-Glückert-Passage 10, 55116 Mainz
www.verbraucherzentrale-rlp.de

Lektorat:
WORDS IN FLOW
Julia Gilcher
Schillerplatz 18, 55116 Mainz
www.wordsinflow.de

Gestaltung:
alles mit Medien
Anke Enders
Freiherr-vom-Stein-Straße 10, 55576 Sprendlingen
www.allesmitmedien.de

Bildnachweis:
Cover: Laura Günther; Portrait Helmut Eiermann: picturepeople Mainz; Portrait: Dr. Julia Gerhards, Maximilian Heitkämper: Laura Günther

Autor*innen:
Dr. Julia Gerhards, Michael Gundall, Maximilian Heitkämper, Jennifer Kaiser und Miriam Raic von der Verbraucherzentrale Rheinland-Pfalz e.V.; Hannah Ballmann und Fabian Geib von der Stiftung MedienKompetenz Forum Südwest; Anja Naumer und Dr. Florian Tremmel von der Medienanstalt Rheinland-Pfalz; Helmut Eiermann, Timo Göth und Sonja Wirtz als Mitarbeiter*innen des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz; Andreas Büsch von der Clearingstelle Medienkompetenz der Deutschen Bischofskonferenz an der KH Mainz.
Ehemalige Autor*innen: Christian Gollner und Barbara Steinhöfel von der Verbraucherzentrale Rheinland-Pfalz e.V.; Christian Wedel und Jeanine Wein, freiberufliche Medienpädagog*innen; Annette Thunemann vom Medienkompetenz Netzwerk Mainz-Rheinhessen.

Diese Lernhilfe wurde erstellt von:

Das Projekt wurde gefördert durch:

Dank:
Wir danken unseren Förderern, die ein solches länderübergreifendes Projekt möglich gemacht haben. Unser Dank gilt auch allen weiteren Multiplikatoren, die uns helfen, dieses Wissen an die interessieren Onliner*innen weiterzutragen.
Ein besonderer Dank gilt zudem allen Autor*innen und Interview-Partner*innen, den Coverfoto-Modellen und allen weiteren Unterstützer*innen des Projekts.

Herausgeber:
Verbraucherzentrale Rheinland-Pfalz e.V.
Seppel-Glückert-Passage 10, 55116 Mainz
www.verbraucherzentrale-rlp.de

Bezugsadressen:
Verbraucherzentrale Rheinland-Pfalz e.V.
Seppel-Glückert-Passage 10, 55116 Mainz
(06131) 28 48 0
www.verbraucherzentrale-rlp.de/smart-surfer

Smart Surfer | 2021